Phishing Defence Service

Defences against phishing often rely exclusively on users being able to spot phishing emails. This approach will only have limited success.

We now have a displaced workforce working from home, and all of the distractions that entails – not spotting the phishing email will cause significant and expensive, long-lasting damage.

CGI's Cyber Analysts deliver our Phishing Defence Service. Providing a powerful defensive capability to ensure your resilience to attacks will improve without disrupting productivity.

We can detect and destroy the Phishing email in your organisation, ensuring the attack has been defended and the business remains operational without disruption.

Awareness is critical for your workforce to ensure our complex phishing exercise campaigns test them. Making sure vigilance remains and recommendations for users, departments are understood to detect and defend against sophisticated attacks.

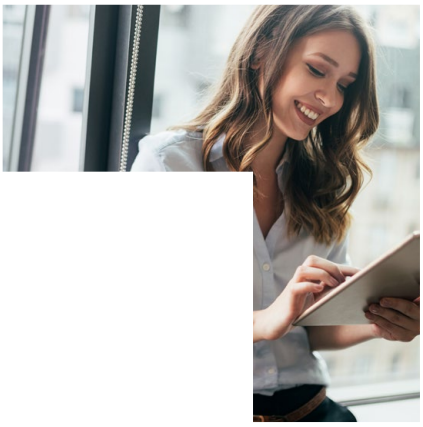
Strengthen your defences

Reporting Button

Identifying who to contact when an unusual email lands in your inbox is one of the critical elements of a successful Phishing Defence Service. The addition of a phishing reporter button to your email toolbar allows for simple, fast reporting. One click and the email leaves your inbox, leaving you feeling secure that you have done the right thing.

Key capabilities:

- Empowers employees with simple reporting.
- Reinforces the reporting message with an immediate reply thanking users and giving additional feedback.
- Deploys easily on PC and MACs. Compatible with Outlook, Microsoft 365, Gmail, or Lotus Notes.
- Preserves the integrity of the email, ensuring the analysts investigating the threat can see headers, URL's and attachments.
- Collects reporting metrics on both the email and the reporter.



Once an email has been identified as malicious, CGI's Vision can be used to find and remove the entire phishing campaign across the whole enterprise swiftly.

Triage

A strong reporting culture is an intelligent tactic for organisations looking to protect themselves from phishing attacks; however, it can create a vast amount of work for the Security Operations Centre (SOC). Our analysts use CGI's Triage to automate and categorise these emails, making it easier and quicker to spot highly malicious threats to an organisation.

Key capabilities:

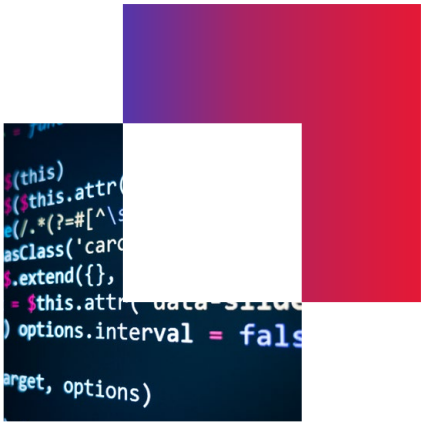
- Automates the identification, prioritisation and remediation of phishing threats in real-time.
- Creates 'Clusters' using a vast library of rules to group emails, speeding up analysis. Clustering also helps to quieten the noise caused by false positives and assists prioritisation.
- Utilises the knowledge of 20 million endpoints by rapidly ingesting the new rules from the wider CGI community
- Identifies previously unseen phishing campaigns allowing our analysts to manually analyse and provide feedback, helping remediate emerging threats.
- Sends employees who report an email motivating feedback to further engagement.
- Provides detailed monthly insight on emails and false positives reported, known malicious malware, phishing simulation and spam.
- Gives feedback on malicious emails promptly to the SOC to facilitate remediation.

Vision

Once an email has been identified as malicious, Vision can be used to find and remove the entire phishing campaign across the whole enterprise swiftly. Vision creates a "search and destroy" capability that provides a fast, proactive response, reducing your organisation's exposure to the threat.

Key capabilities:

- Supports complex queries involving domains, URLs, attachment names and hashes.
- Can find even dangerous polymorphic attacks.
- Quarantines emails with a single click.
- Seamlessly un-quarantines items if no threat is identified, returning them to your employee's inbox.
- Extensively audits and logs all actions, allowing you to understand who is searching for what within your environment and keeps you in compliance.



Some phishing emails get through even the best email gateways and safety nets. Staff must be trained to spot these emails and deal with them effectively. Every month, we provide a phishing simulation training package to create 'human sensors' trained to spot and report malicious emails.

Test your last line of defence

Education

Simulation campaigns

Some phishing emails get through even the best email gateways and safety nets. Staff must be trained to spot these emails and deal with them effectively. Every month, we provide a phishing simulation training package to create 'human sensors' trained to spot and report malicious emails.

Key capabilities:

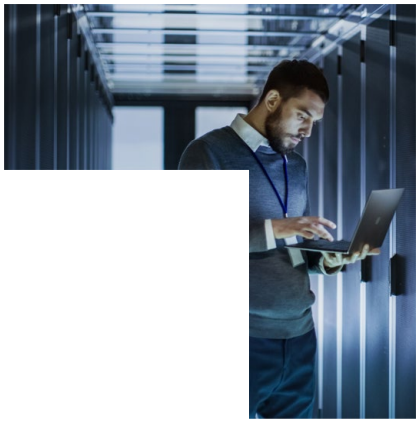
- Educates with real-world scenarios that have been found targeting your organisation.
- Applies your own branding to any activity and allows you to customise using a wide range of themes and content.
- Protects you against threats seen to target your specific industry sector or email gateway.
- Provides monthly reporting detailing your organisation's performance and progress.
- It gives you the ability to target smaller high-risk groups with job-specific scenarios – i.e. finance departments.
- Prepares key targets in your organisation – i.e. CEO, board members with spear-phishing campaigns.

Learning Management System (LMS)

Our analysts use CGI's LMS to create an employee education programme that is tailored alongside the simulations. LMS covers a range of cyber security risks through standalone modules or in conjunction with the simulation campaigns.

Key capabilities:

- Allows you to customise and brand with company logos, etc.
- Keeps employees engaged with interactive animations, videos, quizzes, and gamification.
- Available in over 30 languages.
- Includes standalone modules to provide training in GDPR, HIPAA, Cyber Security of Business and Business Email Compromise (BEC).
- Provides educational pages to reinforce the training of users who interact with a simulation email.
- Enables you to upload any learning materials that your organisation already uses.
- Sends completion tracking and email prompts to complete assigned training modules.
- Provides monthly reporting, including metrics on employee engagement and how prepared your organisation is.



About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industry sectors in 400 locations worldwide, our 77,000 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit cgi.com/uk/cyber-security
Email us at cyber.enquiry.uk@cgi.com